

The operating system used is windows. IDE=PyCharm. Python version 3.7

The library used for target generation is numpy.

The library used for sha256 is hashlib.

The library used for time calculation is time.

The target generation.

Difficulty is the number of zeros present in the first of a binary number.

For target generation the difficulty used at first is d=10

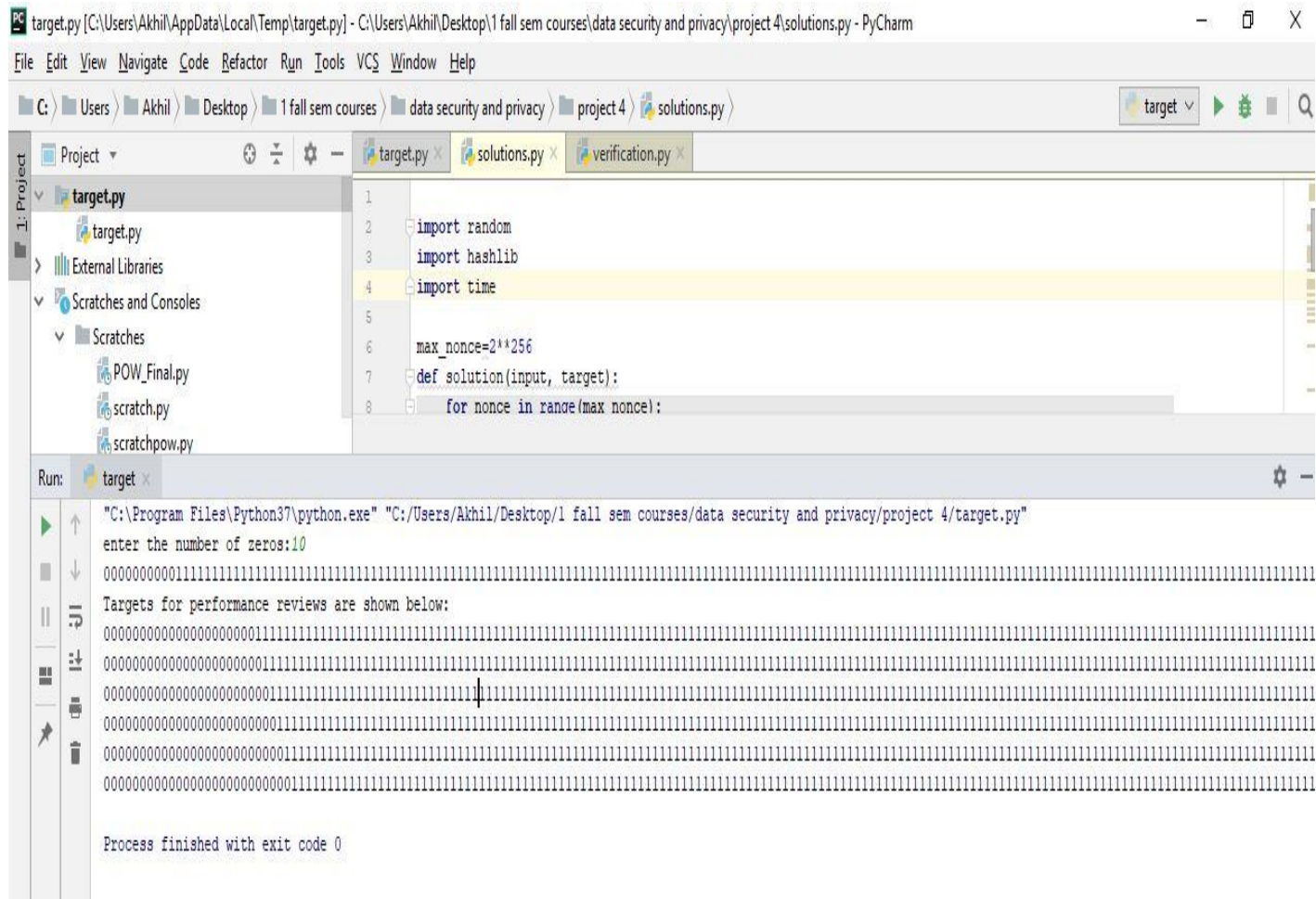
The code used is:

```
import numpy as np
def main():
    no = input("enter the number of zeros:") # to enter no of zeros
    d=int(no)
    first = np.zeros(d, int)
    last = np.ones(256 - d, int)
    f = "".join(map(str, first))
    l = "".join(map(str, last))
    target = f + l #concatenation of two strings
    print(target)
    w1 = open("C:\\Users\\Akhil\\Desktop\\1 fall sem courses\\data security and privacy\\project 4\\target.txt", "w+") #wr
    w1.write(target)
    w1.close()

def main2():
    for no in range (21,27): #to display targets with d from 21 to 26
        d=int(no)
        first = np.zeros(d, int)
        last = np.ones(256 - d, int)
        f = "".join(map(str, first))
        l = "".join(map(str, last))
        target2 = f + l
        print(target2)
        no+=1
        w2 = open("C:\\Users\\Akhil\\Desktop\\1 fall sem courses\\data security and privacy\\project 4\\targetforperformanc
        w2.write(target2)
        w2.close()

if __name__ == "__main__":
    main()
    print("Targets for performance reviews are shown below:")
    main2()
```

The output of d=10 and also d=21,22,23,24,25,26 for performance power review is shown below:



These targets with d=10 is written to file target.txt

The targets with d=21 to 26 is written to file targetforperformance.txt.

Finding Solutions:

The code used is :

```
max_nonce=2**256
def solution(input, target):
    for nonce in range(max_nonce):
        # to create random numbers of 256bit
        i = random.randint(0, pow(2, 256))
        hash_result = hashlib.sha256((str(input) + str(i)).encode('utf-8')) #SHA256encryption
        hex_dig = hash_result.hexdigest() #converting to hexadecimal
        hash_bin = str(bin(int(hex_dig,16))) #converting to binary
        hash_bin=hash_bin[2:]
        hash_10 = int(hash_bin,2) #converting nounce to decimal
        target_10 = int(target,2) #converting target to decimal
        print ('Nounces:',hash_10)
        if hash_10 <= target_10:
            print(" ")
            print('The final hash value or solution is:',i) #solution
            return str(i)
        else:
            i+=1
    if i<= pow(2,256):
        i = 0
```

The code for finding time is:

```
# checkpoint the current time
start_time = time.time()

f = solution(input_in, target_in )
wl = open("C:\\Users\\Akhil\\Desktop\\1 fall sem courses\\data security and privacy\\project 4\\solution.txt", "w+")
wl.write(f)
wl.close()

print(" ")
print("Execution completed")

# checkpoint how long it took to find a result
end_time = time.time()

elapsed_time = end_time - start_time
print("Elapsed Time: %.4f seconds" % elapsed_time)
```

[illegible]

Nounces: 53147078150233032586330354821295307316287203674183785010091526970596544349579
Nounces: 30260915972776288663662227637447049452379649635348561136966368331760564188288
Nounces: 50468570383694941594119522062879536832574441414206543122491400722870501959487
Nounces: 25485945063437910081781413077459557495457713997826959081663835208127620497283
Nounces: 36005643695977435910446733375793317861812519300333192018879779220549526342267
Nounces: 14944724994979583880039974509674182605200122403246511683299882243857911252391
Nounces: 7536873174489396306488387925518870954452856019739322926588950056725880554623
Nounces: 50723922604513829077833583700510841702605230734231747671950356141722673201463
Nounces: 322853703416180587722804652294080576917569905249012949649027797236151332546
Nounces: 44698148181345291189078308964147030250942429387907242881387017113306394272981
Nounces: 92647691606936263294469158140336699749455919050888848010345208366219116630178
Nounces: 110628345207563146283967374036460751222205311933394869337965722969557992834840
Nounces: 98224691703466212731026887298815969946519698229066787384594549319894352277460
Nounces: 12410453815576626208418272072880083479746711543634601338120692835594504636106
Nounces: 10330035284793931162477169944757134162953785566966233424448723342634586628877
Nounces: 91647806424377350060886227233521765190558608618623378794978370234470814719509
Nounces: 29807553637171027816087669324193682958813826633160369744201495334138043465319
Nounces: 80896938019599441776753848993194285116071383909112644296074308930170053030978
Nounces: 36308331870473782108587436719792604909890046874129447643071043599336652809642
Nounces: 6745217007761196156894586486329252386453894969492308364867567932819501893991
Nounces: 78874790230091042364377386489986285015946181466899118621945622845662905243940
Nounces: 39677511340723043688022336015927434174113547033142614969568794509072699631680
Nounces: 39790010787018462702065914301183633709952794978920675723291084637885617748030
Nounces: 11775438352822922515872677196330052905700675196172452471735468741751421191

The final hash value or solution is: 14687154087361411489058732443655953023067053047311230785430994332882182400134

Execution completed

Elapsed Time: 0.0360 seconds

Process finished with exit code 0

The time taken for d=10 is 0.0360 seconds.

The code used is:

The output of verification is:

[illegible]

The performance of system for different d values are shown below, d=21,22,23,24,25,26

D=21

```
solutions x
Nounces: 40903456884480336787222919455211035344838429019100134813141736374825969287507
Nounces: 91572056361979426725415693030696905371122145610669420555518888948862969815173
Nounces: 19810613150857414506540867534230507042744346990964314562807726508253836410607
Nounces: 57745212406518566268649464016469121572254327812237868699012836175247447275215
Nounces: 16423292878815440171932160206348961434153773493411321294384504564335507604612
Nounces: 44946408331406886988920142935726873359635184484008951561671685339529305468402
Nounces: 81943639216806069088698442357380188243058973550929295365191944003083022000852
Nounces: 15068286075510562693339870330511191738751534896036604534298921863783914594747
Nounces: 18652049101850745492472394557753850611480614430223913530723431000937130487659
Nounces: 105126295558622650699632734326499979586088658549022363515124241303083771061157
Nounces: 101888007280184336759679620131454806452848900595589795855356497806843992356627
Nounces: 13676070073066554553871844133372173458914120150595519630318846330142456318481
Nounces: 52283802622877896159521834966934101890960426801493971363969378552824939165851
Nounces: 33547316546298453838555674064872009479945507314870682985421596110843431853652
Nounces: 29305344440854976280843933214785291185386644180260772904698456207436597740198
Nounces: 108963084132333800217462694748073296579699987134079216274903561673030995754537
Nounces: 4756893212559705938999244043247430235364635630846966113802283696331035927918
Nounces: 106196606579122841703887017951117707307609329673834866600364026016711837752365
Nounces: 31871354530676144130282837112043634524878717041711481933828336020087851

The final hash value or solution is: 872061650422780564800831429103331426152535542580765702063044873747716685779

Execution completed
Elapsed Time: 85.9166 seconds
```

Time took =85.9166 seconds.

D=22, Time took=238.7570 seconds.

```
Nounces: 104185925436466040304578517324454338891603496019456571072917323214461995691167
Nounces: 11154318675205488730345327667721597322609356999965633635042481584872314608090
Nounces: 22315244246644892407706092320627071012229858691464239832268833756944148318002
Nounces: 29865716884104402864647793730450175872920174243185457496041661963017463987886
Nounces: 13396511901491098789052251437230740030441022048350531070853733203285971

The final hash value or solution is: 1712264735709226721144155997731546737473978590664541481893510505334741578633

Execution completed
Elapsed Time: 238.7570 seconds

Process finished with exit code 0
```


D=23, Time took = 743.3135 seconds

Nouns: 4932432858965552005997022723490522703698457210832144439078317413619572057871
Nouns: 19547342950479288387096794744792165211037138503183553894802375110454638427018
Nouns: 69979775893981397743440941575746555145861397439915507410339259337677158574025
Nouns: 44482526383472977438238581254961896985923750206342912238547754956853408808794
Nouns: 62994343467040357188691624107193782516212849527489867671850869745091981855344
Nouns: 112777924578176300425215114530207707224273665085608977774526398216241771352446
Nouns: 97157794455380908341147848236480617999796232903732228790627451184060312473033
Nouns: 67321536778438310394662695109154690704765140637938885777798447132230185209519
Nouns: 11701184223125276791246792406782324249596988648977861855717844520729495

The final hash value or solution is: 98110347199608213301183166830559111296315860629531944500247259257593734948668

Execution completed

Elapsed Time: 743.3135 seconds

```
Process finished with exit code 0
```

D=24 , Time took=1235.5470 seconds.

Nounces: 49631116902963472317065203292219202141353378173668458030162201360448587503026
Nounces: 49722537750944082047263962864711516871787978532941235613279114476340190385785
Nounces: 64605983110842374892298088429792144248105208404951242813109838959278718472396
Nounces: 13294187780259150155534824349565136987698565943581214456225597409235406042166
Nounces: 18024631978556548787835243415907244439255190042645541944736141280287478228667
Nounces: 21387719832232327773077080678161118426316276709949729706327633234295990947074
Nounces: 51034527966188453142303280809703319715683493283080216959920118557692122710409
Nounces: 71254976334098570404310825735413339296134806473046285427833788245464044757065
Nounces: 1477355859305254615699397804768519635855124788652858852754374444323749296091
Nounces: 5932768761487587705893073609673661571668550056398496753842434003368395

The final hash value or solution is: 101596638025311214286375826054828575876338172081204744453480688703201686201731

Execution completed

Elapsed Time: 1235.5470 seconds

```
Process finished with exit code 0
```

D=25, Time took =2924.0309 seconds .

19061106Z: 00 / 10007700000000000000007 / 20000 / 7000270000100000000000 / 000 / 00 / 71707000

The final hash value or solution is: 27396551519002561544647835296187181719263757514096782167752552779698811166944

Execution completed

Elapsed Time: 2924.0309 seconds

Process finished with exit code 0

